

**PURPOSE**

To ensure the continued integrity of Michigan Department of Health and Human Services (MDHHS) information systems through processes to initialize, change, monitor, and maintain secure configurations throughout their life cycle.

**REVISION HISTORY**

Issued: 6/01/2021.  
Next Review: 6/01/2022.

**DEFINITIONS****Authorization Boundary**

All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

**Baseline Configuration**

A set of specifications for a system, or cybersecurity and infrastructure (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

**Confidential Information**

Information of a private nature that is protected by law from public disclosure, such as identifiable health information and social security numbers.

**Configuration Control Board (CCB)**

A group of qualified people with responsibility for the process of controlling and approving changes throughout the development and operational lifecycle of products and systems; see Enterprise Change Advisory Board in [DTMB 1340.00.060.01, Configuration Management Standard](#).

**Configuration Item**

An identifiable part of a system (such as hardware, software, firmware, documentation, or a combination thereof) that is a discrete target of configuration control processes.

## **Configuration Management**

Configuration Management (CM) comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.

### **Configuration Management (CM) Plan**

A comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems.

### **Personally Identifiable Information (PII)**

Confidential information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

### **Workforce Member**

Includes full and part-time employees, affiliates, associates, students, volunteers, contractors, and staff from third party entities.

## **POLICY**

Information systems are typically in a constant state of change in response to new, enhanced, corrected, or updated hardware and software capabilities, patches for correcting software flaws and other errors to existing components, new security threats, and changing business functions. Configuration changes must be managed through controls that protect systems and the lines of business they support from loss of confidentiality, integrity, or availability.

MDHHS must:

- Establish and maintain baseline configurations and inventories of information systems, including hardware, software, firmware, and documentation, throughout the system development life cycle (SDLC).
- Establish and enforce security configuration settings for information technology products employed in organizational systems.

In compliance with [Department of Technology, Management and Budget \(DTMB\) 1340.00, Information Technology Information Security Policy](#), MDHHS must ensure implementation of all moderate baseline security controls catalogued in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) from the NIST Computer Security Resource Center. This policy sets forth requirements from the configuration management [CM] family of NIST controls managed by MDHHS in accordance with [DTMB 1340.00.060.01, Configuration Management Standard](#). MDHHS must review this policy annually.

Where applicable, this policy requires compliance with other federal and state laws, rules and regulations, policies, standards or other guidelines, including but not limited to the following:

- Centers for Medicare and Medicaid Services (CMS) Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)
- Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy
- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities
- Social Security Administration (SSA) Technical System Security Requirements (TSSR)
- U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and Part 164, Subparts A and C

### **Baseline Configuration [CM-2]**

MDHHS must develop, document, and maintain, under configuration control, a current baseline configuration of each information system.

### **Reviews and Updates [CM-2(1)]**

MDHHS must review and update the baseline configuration of each information system:

- Annually, at a minimum.

- When configuration settings change due to critical security patches, upgrades, emergency changes and major system changes/upgrades.
- As an integral part of information system component installations and upgrades.
- Supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy.

**Retention of Previous Configurations [CM-2(3)]**

MDHHS must retain previous versions of baseline configurations of the information system to support rollback.

**Configuration Change Control [CM-3]**

MDHHS must coordinate and provide oversight of configuration change control activities conducted through the DTMB Enterprise Change Advisory Board.

**Test / Validate / Document Changes [CM-3(2)]**

MDHHS must test, validate, and document changes to the information system before implementing changes on the operational system.

**Security Impact Analysis [CM-4]**

MDHHS must analyze changes to the information system to determine potential security impacts prior to change implementation.

**Separate Test Environment [CM-4(1)]**

Where required based on data classification, MDHHS must:

- Maintain separate development/test environments and analyze changes to the information system in a separate test environment before implementation in an operational environment.
- Prohibit processing or storing of Personally Identifiable Information (PII) in test environments.

**Security Impact Analysis / Separate Test Environment [CM-4(2)]**

Where required based on data classification, MDHHS must check the security functions after the information system is changed to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome for meeting the system's security requirements.

**Access Restrictions for Change [CM-5]**

MDHHS must define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

**Automated Access Enforcement/Auditing [CM-5(1)]**

Where required based on data classification, MDHHS must employ automated mechanisms to enforce access restrictions to configuration change information and support auditing of the enforcement actions.

**Limit Production /Operational Privileges [CM-5(5)]**

Where required based on data classification, MDHHS must:

- Limit privileges to change information system components and system-related information within a production or operational environment]
- Review and reevaluate privileges at least quarterly.

**Configuration Settings [CM-6]**

MDHHS must:

- Establish and document configuration settings for information technology products employed within the information system using security configuration checklists that reflect the most restrictive mode consistent with operational requirements.
- Implement the configuration settings.
- Identify, document, and approve any deviations from established configuration settings for information system components based on operational requirements.

- Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

**Least Functionality [CM-7]**

MDHHS must:

- Configure the information system to provide only essential capabilities.
- Specifically prohibit or restrict the use of functions, ports, protocols, and/or services that are not required for the business function of the information system.

**Periodic Review [CM-7(1)]**

MDHHS must:

- Review the information system at least annually to identify unnecessary and/or nonsecure functions, ports, protocols, and services.
- Disable unnecessary and/or nonsecure functions, ports, protocols, and services within the information system.

**Information Systems Component Inventory [CM-8]**

MDHHS must develop and document an inventory of information system components that:

- Accurately reflects the current information system.
- Includes all components within the authorization boundary of the information system.

**Configuration Management Plan [CM-9]**

MDHHS must develop, document, and implement a configuration management plan for the information system that:

- Addresses roles, responsibilities, and configuration management processes and procedures.
- Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.

- Defines the configuration items for the information system and places the configuration items under configuration management.
- Protects the configuration management plan from unauthorized disclosure and modification.

**Software Usage Restrictions [CM-10]**

MDHHS must track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

**Open Source Software [CM-10(1)]**

MDHHS must establish restrictions on the use of open source software. Open source software must:

- Be legally licensed
- Approved by DTMB.
- Adhere to a security configuration baseline checklist from the U.S. Government or industry.

**User-Installed Software [CM-11]**

MDHHS must

- Enforce enterprise policies governing the installation of software by users through automated methods.
- Monitor policy compliance at least annually.

**ROLES AND RESPONSIBILITIES:**

The MDHHS security officer and privacy officer must determine roles and responsibilities for Compliance and Data Governance Bureau personnel to support implementation of this policy.

MDHHS workforce members are responsible for reading, understanding, and complying with policies, standards, and procedures based on access controls.

**ENFORCEMENT**

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

## REFERENCES

### Federal Standards/Regulations:

NIST 800-53 rev.4:

CM-1 Configuration Management Policy and Procedures

CM-2 Baseline Configuration and System Component Inventory

CM-2(1) Reviews and Updates

CM-2(3) Retention of Previous Configurations

CM-3 Configuration Change Control

CM-3(2) Test / Validate / Document Changes

CM-4 Security Impact Analysis

CM-4(1) Separate Test Environment

CM-4(2) Security Impact Analysis / Separate Test Environment

CM-5 Access Restrictions for Change

CM-5(1) Automated Access Enforcement/Auditing

CM-5(5) Limit Production /Operational Privileges

CM-6 Configuration Settings

CM-7 Least Functionality

CM-7(1) Periodic Review

CM-8 Information Systems Component Inventory

CM-9 Configuration Management Plan

CM-10 Software Usage Restrictions

CM-10(1) Open Source Software

CM-11 User-Installed Software

45 CFR §164.310(d)

45 CFR §164.310(d)(1) Device and Media Controls (R)

45 CFR §164.310(d)(2)(iii) Accountability (A)

### State Standards/Regulations:

[MDHHS Policy Manuals](#)

[68E-250 Workstation Security Policy and Procedure](#)

[68E-260 Accountability Policy and Procedure](#)

[DTMB Administrative Guide](#)

[IT Technical Policies, Standards and Procedures](#)

[1340.00.060.01 Configuration Management Standard](#)  
[1340.00.060.04 Enterprise Change Control Process Standard](#)

## CONTACT

For additional information concerning this policy, contact the MDHHS Compliance and Data Governance Bureau at [MDHHSPrivacySecurity@michigan.gov](mailto:MDHHSPrivacySecurity@michigan.gov).